PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-268777
(43)Date of publication of application : 22.09.1994

(51)Int.CI. H04M 15/00
H04B 7/26
H04L 9/00
H04L 9/10
H04L 9/12
H04Q 7/04

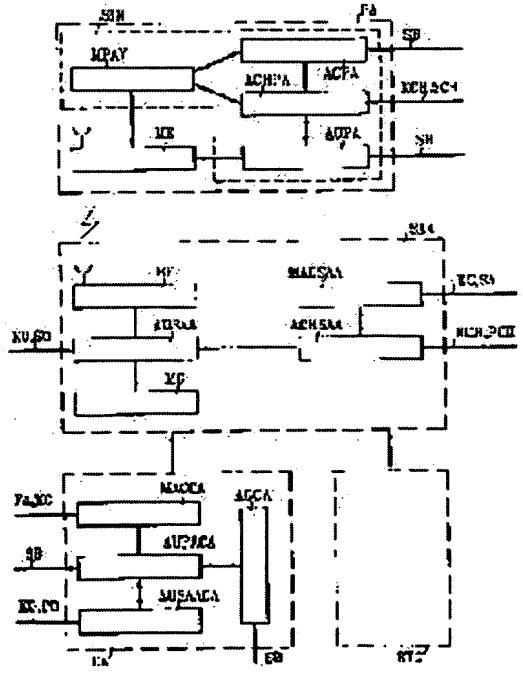
(21)Application number : 05-235086
(22)Date of filing : 21.09.1993

(71)Applicant : FR TELECOM
LA POSTE
(72)Inventor : NEVOUX ROLA
HIOLLE PHILIPPE

(30)Priority
Priority number : 92 9211223 Priority date : 21.09.1992 Priority country : FR

(54) LONG-DISTANCE COMMUNICATION FACILITY HAVING PREPAYMENT MEANS TO BE SAFELY REMOTE LOADED AND REMOTE LOADING METHOD FOR THE FACILITY

(57)Abstract:
PURPOSE: To secure both secrecy and maintenance for a remote loading method of value unit for prepayment.
CONSTITUTION: This facility includes an active authentication mode of an independent set (PA) and an access system (SAA), a calculation mode of a remote loading master key (KCH or (SCH, PCH)) set at the level of a certification center (CA), a transmission mode set to the access system (SAA) of an enciphered remote loading master key, and a remote loading mode that offers a safe remote loading method of a prepayment means (MPAY) to be executed by the access system with the help of the remote loading master key that is transmitted in the said way respectively in response to a prescribed number of remote loading request words (R) of value units which are given from the set (PA).



LEGAL STATUS
[Date of request for examination] 14.09.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－268777

(43)公開日　平成６年(1994)９月22日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
H04M 15/00		G 7190-5K		
		Z 7190-5K		
H04B 7/26	109	S 7304-5K		
H04L 9/00				
9/10				

審査請求　未請求　請求項の数15　ＯＬ　（全16頁）　最終頁に続く

(21)出願番号　特願平5－235086

(22)出願日　平成５年(1993)９月21日

(31)優先権主張番号　９２１１２２３

(32)優先日　1992年９月21日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591034154
フランス・テレコム
ＦＲＡＮＣＥ　ＴＥＬＥＣＯＭ
フランス国、75015　パリ、プラス・ダルレ、６

(71)出願人　592132006
ラ・ポスト
ＬＡ　ＰＯＳＴＥ
フランス国、75027　パリ・セデ、アベニュ・ド・セグール、20

(74)代理人　弁理士　筒井　大和　（外２名）

最終頁に続く

(54)【発明の名称】安全に遠隔ローディングされる前払い手段を備えた遠距離通信設備およびその遠隔ローディング方法

(57)【要約】

【目的】　前払い用の価値単位の遠隔ローディングの秘密性および保全性を確保する。

【構成】　本設備は、独立セット（ＰＡ）から発せられる所定の数の価値単位の遠隔ローディング要請ワード（Ｒ）に応じて：－独立セット（ＰＡ）およびアクセス・システム（ＳＡＡ）の能動的な認証；－認可センター（ＣＡ）のレベルでの遠隔ローディング・マスターキー（ＫＣＨあるいは（ＳＣＨ，ＰＣＨ））の計算；－暗号化された遠隔ローディング・マスターキーのアクセス・システム（ＳＡＡ）へ向けた送信；－このように送信された遠隔ローディング・マスターキーの助けを得てアクセス・システムにより行なわれる前払い手段（ＭＰＡＹ）の安全な遠隔ローディング、が提供される遠隔ローディング・モードを含む。

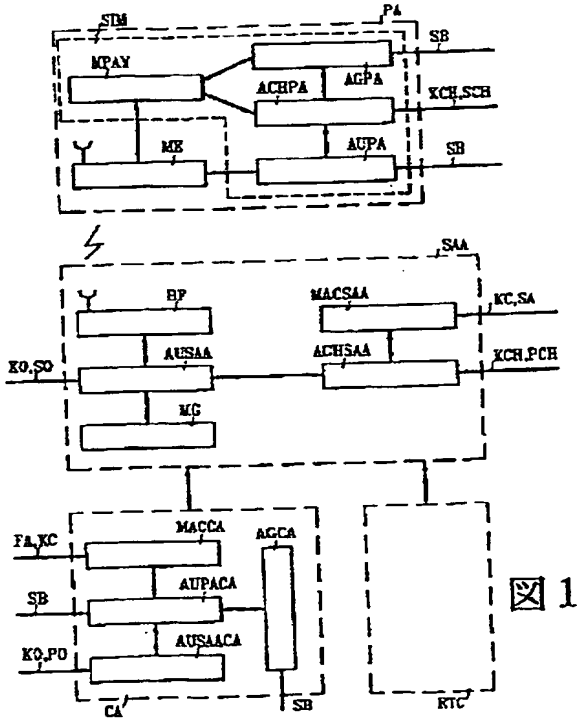


図１

【特許請求の範囲】

【請求項１】　遠距離通信設備で、次のもの、すなわち：

－少なくとも一つの交換電話ネットワーク（ＲＴＣ）；

－自立電話加入者アクセス・システム（ＳＡＡ）で、次のもの、すなわち：

・前記交換電話ネットワークに連結された少なくとも一つのベース局（ＢＦ）；

・前記ベース局に接続され、前記交換電話ネットワーク（ＲＴＣ）の有料サービスの利用に対する料金を計算することができる料金計測手段（ＭＧ）を含む、操作手段；

・格納マスターキー（ＫＣあるいはＦＡ）の助けを得て暗号関数（ＡＣあるいはＦＣ）を確立することができる第一の暗号化／復号手段（ＭＡＣＳＡＡ）；

を有するアクセス・システム（ＳＡＡ）；

－少なくとも一つの独立セット（ＰＡ）で、次のもの、すなわち：

・前記ベース局（ＢＦ）と相互通信を確立することができる手段；

・前記料金計測手段により計算され送信される利用料金を支払うために用いられる価値単位を収容することができる前払い手段（ＭＰＡＹ）；

・各加入者に固有の所定のセット・ベース・マスターキー（ＳＢ）の助けを得て認証関数（Ａ）を確立することができる第一のセット認証手段（ＡＵＰＡ）；

を含む独立セット（ＰＡ）；

－認可センター（ＣＡ）であって、次のもの、すなわち：

・前記格納マスターキー（ＫＣあるいはＦＡ）の助けを得て暗号化／復号関数（ＡＣあるいはＦＣ）を確立することができる第二の暗号化／復号手段（ＭＡＣＣＡ）；

・前記セット・ベース・マスターキー（ＳＢ）の助けを得てセット認証関数（Ａ）を確立することができる第二のセット認証手段（ＡＵＰＡＣＡ）；

を有する認可センター（ＣＡ）；

からなる遠距離通信設備であって、

前記独立セット（ＰＡ）が、更に：

－前記セット・ベース・マスターキー（ＳＢ）の助けを得て生成関数（ＡＧ）を確立することができる第一の生成手段（ＡＧＰＡ）；

－前記セット・ベース・マスターキー（ＳＢ）の助けによって前記生成関数（ＡＧ）による所定のワードの変換として得られた遠隔ローディング・マスターキー（ＫＣＨあるいはＳＣＨ）の助けを得て遠隔ローディング関数（ＡＣＨあるいはＳＣＨ）を確立することができる第一の遠隔ローディング手段（ＡＣＨＰＡ）；

を有し、

前記アクセス・システム（ＳＡＡ）が、更に：

－所定のシステム・ベース・マスターキー（ＫＯあるいはＳＯ）の助けを得てシステム認証関数（ＡＯあるいはＦＯ）を確立することができる第一のシステム認証手段（ＡＵＳＡＡ）；

－所定の数の価値単位を発行することができ、また、前記遠隔ローディング・マスターキー（ＫＣＨあるいはＰＣＨ）の助けを得て遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）を確立することができる第二の遠隔ローディング手段（ＡＣＨＳＡＡ）；

を有し、

前記認可センター（ＣＡ）が、更に：

－前記システム・ベース・マスターキー（ＫＯあるいはＰＯ）の助けを得てシステム認証関数（ＡＯあるいはＦＯ）を確立することができる第二のシステム認証手段（ＡＵＳＡＡＣＡ）；そして、

－前記セット・ベース・マスターキー（ＳＢ）の助けを得て生成関数（ＡＧあるいはＦＧ）を確立することができる第二の生成手段（ＡＧＣＡ）；

を有し、

本遠距離通信設備が、更に、遠隔ローディング・モードを有し、該遠隔ローディング・モードにおいては、前記独立セット（ＰＡ）から発せられる所定の数の価値単位に関する遠隔ローディング要請ワード（Ｒ）に応じて、前記第一および第二のセット認証手段（ＡＵＰＡおよびＡＵＰＡＣＡ）ならびに前記第一および第二のシステム認証手段（ＡＵＳＡＡおよびＡＵＳＡＡＣＡ）が、それぞれ前記アクセス・システムから発せられるセット認証ワード（Ｒ０）と、前記セット・ベース・マスターキー（ＳＢ）の助けを得て前記セット認証関数（Ａ）により得られる該ワード（Ｒ０）の変換（ＲＥＳ０）とを交換し、また、前記認可センター（ＣＡ）から発せられるシステム認証ワード（Ｒ２）と、前記システム・ベース・マスターキー（ＫＯあるいはＳＯ）の助けを得て前記システム認証関数（ＡＯあるいはＦＯ）により得られる該ワード（Ｒ２）の変換（ＲＥＳ２）とを交換することにより、該独立セットおよび該アクセス・システムのそれぞれの能動的認証を実行し、

前記アクセス・システムおよび前記独立セットの認証がチェックされる場合、前記認可センター（ＣＡ）のレベルで前記第二の生成手段（ＡＧＣＡ）が、前記セット・ベース・マスターキー（ＳＢ）の助けを得て前記生成関数（ＡＧ）により遠隔ローディング要請ワードの変換として得られる遠隔ローディング・マスターキー（ＫＣＨあるいは（ＳＣＨ，ＰＣＨ））を計算し、

前記遠隔ローディング・マスターキーが前記認可センターで生成される場合、前記第二の暗号化／復号手段（ＭＡＣＣＡ）が前記格納マスターキー（ＫＣあるいはＦＡ）の助けを得て暗号化されたローディング・マスターキー（ＥＫＣＨあるいはＥＰＣＨ）を前記第一の暗号化／復号手段（ＭＡＣＳＡＡ）に送信し、該第一の暗号化／復号手段はアクセス・システム（ＳＡＡ）のレベルで

格納するためにそれを復号し、

遠隔ローディング・マスターキーが該アクセス・システム（ＳＡＡ）に格納される場合には、安全な方法で価値単位の数（ｎ）を前払い手段に遠隔ロードする目的で、第一および第二の遠隔ローディング手段（ＡＣＨＳＡＡおよびＡＣＨＰＡ）が遠隔ロードされるべき価値単位の数（ｎ）に対する遠隔ローディング要請ワード（Ｒ）、ならびに、遠隔ローディング・マスターキー（ＫＣＨあるいは（ＳＣＨ，ＰＣＨ））の助けを得てなされる該遠隔ローディング要請ワード（Ｒ）の遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）による変換（ＲＥＳ）、を交換する、ものであることを特徴とする遠距離通信設備。

【請求項２】　前記遠隔ローディング要請ワード（Ｒ）およびその変換（ＲＥＳ）を交換する前に、遠隔ローディング依頼の認可を認証する目的で、第一および第二のシステム認証手段（ＡＵＳＡＡおよびＡＵＳＡＡＣＡ）が、認可認証ワード（Ｒ１）および、システム認証マスターキー（ＫＯあるいは（ＰＯ，ＳＯ））助けを得てシステム認証関数（ＡＯあるいはＦＯ）により得られる該認可認証ワードの変換（ＲＥＳ１）を交換することを特徴とする請求項１の設備。

【請求項３】　前記遠隔ローディング要請ワード（Ｒ）およびその変換（ＲＥＳ）の交換と同時に、遠隔ローディング依頼の受信を認証する目的で、第一および第二の遠隔ローディング手段（ＡＣＨＳＡＡおよびＡＣＨＰＡ）が受信認証ワード（Ｒ２）、および、遠隔ローディング・マスターキー（ＫＣＨあるいは（ＰＣＨ，ＳＣＨ））の助けを得て遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）によりなされる該受信認証ワード（Ｒ２）の変換（ＲＥＳ２）を交換することを特徴とする請求項１および２のいずれか１項の設備。

【請求項４】　前記セット認証関数（Ａ）、前記システム認証関数（ＡＯ、ＦＯ）、前記暗号化／復号関数（ＡＣ、ＦＣ）、前記生成関数（ＡＧ）あるいは前記遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）がＤＥＳあるいはＲＳＡタイプの暗号アルゴリズムであることを特徴とする請求項１ないし３のいずれか１項の設備。

【請求項５】　前記前払い手段（ＭＰＡＹ）の遠隔ローディングの手続きが通信中にリアルタイムで生じることを特徴とする請求項１ないし４のいずれか１項の設備。

【請求項６】　前記前払い手段（ＭＰＡＹ）の遠隔ローディングの手続きが、呼び出しが確立する前に、加入者の要請であるいはネットワークの主導で生じることを特徴とする請求項１ないし４のいずれか１項の設備。

【請求項７】　前記前払い手段（ＭＰＡＹ）、第一の遠隔ローディング手段（ＡＣＨＰＡ）、第一の生成手段（ＡＧＰＡ）および第一のセット認証手段（ＡＵＰＡ）が、無線相互通信を確立するための手段（ＭＥ）と協働することができる着脱可能な加入者識別モジュール（ＳＩＭ）に収納されていることを特徴とする請求項１ないし６のいずれか１項の設備。

【請求項８】　前記加入者識別モジュールが、外界からのふさわしくない時期になされるデータの書き込みに対して保護されてまた価値単位を収容することができるメモリ、および該価値単位の助けにより利用料金を支払い、また遠隔ロードされた価値単位の助けによりメモリを再ロードすることができる処理装置を有していることを特徴とする請求項１ないし７のいずれか１項の設備。

【請求項９】　前記加入者識別モジュール（ＳＩＭ）が標準的なＩＳＯタイプのカードに収容され、前記無線相互通信を確立するための手段（ＭＥ）が該カードを読み取るための読み取り装置を有していることを特徴とする請求項１ないし８のいずれか１項の設備。

【請求項１０】　前記加入者識別モジュールが、前記無線相互通信を確立するための手段（ＭＥ）に差し込むことができる機械的なインタフェースを有していることを特徴とする請求項１ないし８のいずれか１項の設備。

【請求項１１】　前記独立セットおよび前記ベース局との間の相互通信が無線あるいは有線によりなされることを特徴とする請求項１ないし１０のいずれか１項の設備。

【請求項１２】　前記独立セットが移動可能あるいは固定式で、個人用あるいは公衆用のものであることを特徴とする請求項１ないし１１のいずれか１項の設備。

【請求項１３】　前払い手段の安全な遠隔ローディングのための方法であって、次のステップ、すなわち：

－ａ）少なくとも一つの交換電話ネットワーク（ＲＴＣ）を提供し；

－ｂ）自立的な電話加入者アクセス・システム（ＳＡＡ）であって、次のもの、すなわち：

・ｂ１）前記交換電話ネットワークに連結された少なくとも一つのベース局（ＢＦ）

・ｂ２）該ベース局に連結された操作手段であって、前記交換電話ネットワーク（ＲＴＣ）の有料サービスの利用に対する料金を計算することができる料金計測手段（ＭＧ）を有する、操作手段、

を有するアクセス・システム（ＳＡＡ）を提供し；

－ｃ）少なくとも一つの独立セット（ＰＡ）であって、次のもの、すなわち：

・ｃ１）前記ベース局（ＢＦ）との相互通信を確立することのできる手段；

・ｃ２）前記料金計測手段により計算され送信される利用料金を支払うための価値単位を収容することができる前払い手段（ＭＰＡＹ）；

・ｃ３）各加入者に固有な所定のセット・ベース・マスターキー（ＳＢ）の助けにより認証関数（Ａ）を確立することができる第一のセット認証手段（ＡＵＰＡ）；

を有する少なくとも一つの独立セット（ＰＡ）を提供し；

－ｄ）認可センター（ＣＡ）であって、次のもの、すなわち：

・ｄ１）格納マスターキー（ＫＣあるいはＦＡ）の助けにより暗号化／復号関数（ＡＣあるいはＦＣ）を確立することができる第二の暗号化／復号手段（ＭＡＣＣＡ）；

・ｄ２）セット・ベース・マスターキー（ＳＢ）の助けによりセット認証関数（Ａ）を確立することができる第二のセット認証手段（ＡＵＰＡＣＡ）；

を有する認可センター（ＣＡ）を提供する；

ステップからなる方法であって、

前記独立セット（ＰＡ）に対し次の備え、すなわち：

－前記セット・ベース・マスターキー（ＳＢ）の助けにより生成関数（ＡＧ）を確立することができる第一の生成手段（ＡＧＰＡ）；そして、－前記セット・ベース・マスターキー（ＳＢ）の助けにより前記生成関数（ＡＧ）により所定のワードの変換として得られる遠隔ローディング・マスターキー（ＫＣＨあるいはＳＣＨ）の助けにより、遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）を確立することができる第一の遠隔ローディング手段（ＡＣＨＰＡ）；

の備えが更に提供され；

前記アクセス・システム（ＳＡＡ）に対し次の備え、すなわち：

－所定のシステム・ベース・マスターキー（ＫＯあるいはＳＯ）の助けによりシステム認証関数（ＡＯあるいはＦＯ）を確立することができる第一のシステム認証手段（ＡＵＳＡＡ）；そして

－所定の数の価値単位を発行することができ、また、遠隔ローディング・マスターキー（ＫＣＨあるいはＰＣＨ）の助けにより遠隔ローディング関数（ＡＣＨあるいはＳＣＨ）を確立することができる第二の遠隔ローディング手段（ＡＣＨＳＡＡ）；

の備えが更に提供され；

前記認可センター（ＣＡ）に対し次の備え、すなわち：

－前記システム・ベース・マスターキー（ＫＯあるいはＰＯ）の助けによりシステム認証関数（ＡＯあるいはＦＯ）を確立することができる第二のシステム認証手段（ＡＵＳＡＡＣＡ）；そして

－前記セット・ベース・マスターキー（ＳＢ）の助けにより生成関数（ＡＧ）を確立することができる第二の生成手段（ＡＧＣＡ）；

の備えが更に提供され；本方法が、更に、遠隔ローディング・ステップを含み、該ステップにおいては、前記独立セット（ＰＡ）から発せられる所定の数の価値単位に関する遠隔ローディング要請ワード（Ｒ）に応じて、第一および第二のセット認証手段（ＡＵＰＡおよびＡＵＰＡＣＡ）ならびに第一および第二のシステム認証手段（ＡＵＳＡＡおよびＡＵＳＡＡＣＡ）が、それぞれ前記アクセス・システムから発生されるセット認証ワード

（Ｒ０）と、セット・ベース・マスターキー（ＳＢ）の助けを得てなさせる該セット認証ワードのセット認証関数（Ａ）による変換（ＲＥＳ０）とを交換し、また、前記認可センター（ＣＡ）から発せられるシステム認証ワード（Ｒ２）と、システム・ベース・マスターキー（ＫＯあるいはＳＯ）の助けを得てなされる該システム認証ワード（Ｒ２）のシステム認証関数（ＡＯあるいはＦＯ）による変換（ＲＥＳ２）とを交換することにより、前記独立セットおよび前記アクセス・システムのそれぞれの能動的認証を実行し；アクセス・システムおよび独立セットの認証がチェックされる場合、第二の生成手段（ＡＧＣＡ）が認可センター（ＣＡ）のレベルで、セット・ベース・マスターキーの助けを得てなされる遠隔ローディング要請ワードの生成関数（ＡＧ）による変換である遠隔ローディング・マスターキー（ＫＣＨあるいは（ＳＣＨ，ＰＣＨ））を計算し；遠隔ローディング・マスターキーが前記認可センターのレベルで生成される場合には、第二の暗号化／復号手段（ＭＡＣＣＡ）が、格納マスターキー（ＫＣあるいはＦＡ）の助けを得て暗号化されたローディング／マスターキー（ＥＫＣＨあるいはＥＰＣＨ）を第一の暗号化／復号手段（ＭＡＣＳＡＡ）に送信し、該第一の暗号化／復号手段（ＭＡＣＳＡＡ）はアクセス・システム（ＳＡＡ）のレベルで格納する目的でそれを復号し；遠隔ローディング・マスターキーをアクセス・システム（ＳＡＡ）に格納する場合には、第一および第二の遠隔ローディング手段（ＡＣＨＳＡＡおよびＡＣＨＰＡ）が、安全な方法で価値単位の数（ｎ）を遠隔ローディングする目的で、遠隔ロードされるべき価値単位の数（ｎ）に対する遠隔ローディング要請ワード（Ｒ）、および、遠隔ローディング・マスターキー（ＫＣＨあるいは（ＰＣＨ，ＳＣＨ））の助けを得てなされる該遠隔ローディング要請ワードの遠隔ローディング関数（ＡＣＨあるいは（ＦＣＨ））による変換（ＲＥＳ）、を交換する；ことを特徴とする、前払い手段の安全な遠隔ローディングのための方法。

【請求項１４】　前記遠隔ローディング要請ワード（Ｒ）およびその変換（ＲＥＳ）を交換する前に、遠隔ローディング依頼の認可を認証する目的で、第一および第二のシステム認証手段（ＡＵＳＡＡおよびＡＵＳＡＡＣＡ）が認可認証ワード（Ｒ１）、およびシステム認証マスターキー（ＫＯあるいは（ＳＯ，ＰＯ））の助けを得てシステム認証関数（ＡＯあるいはＦＯ）により得られる該認可認証ワードの変換（ＲＥＳ１）を交換することを特徴とする請求項１３の方法。

【請求項１５】　前記遠隔ローディング要請ワード（Ｒ）およびその変換（ＲＥＳ）を交換すると同時に、前記遠隔ローディング依頼の受信の認証を目的として、第一および第二の遠隔ローディング手段（ＡＣＨＳＡＡおよびＡＣＨＰＡ）が受信認証ワード（Ｒ２）、および、遠隔ローディング・マスターキー（ＫＣＨあるいは

（ＰＣＨ，ＳＣＨ））の助けを得て遠隔ローディング関数（ＡＣＨあるいはＦＣＨ）によりなされる該受信認証ワード（Ｒ２）の変換（ＲＥＳ２）を交換することを特徴とする請求項１３および１４のいずれか１項の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、前払い手段の安全な遠隔充填（ローディング）に関するものである。

【０００２】本発明は遠距離通信に一般的に適用でき、特に、「移動通信のための広域システム（ＧＳＭ、GLOBAL SYSTEM FOR MOBILE COMMUNICATION）」と呼ばれる、９００Ｈｚで運営される公衆車両との通信のためのディジタル・システムに適用できる。

【０００３】

【従来の技術】知られているように、遠距離通信の設備は次のものを含んでいる：

－少なくとも一つの交換電話ネットワーク；

－次のものを含む独立電話加入者アクセス・システム；

・前記交換電話ネットワークに連結された少なくとも一つのベース局（基地局）；

・前記ベース局に連結された操作手段であって、前記交換電話ネットワークの有料サービスの利用に対する料金を計算することのできる料金計測手段を含む、操作手段；

・格納マスターキーの助けを得て暗号関数を実現することができる第一の暗号化／復号手段；

－次のものを含む少なくとも一つの独立セット（独立通信機）；

・前記ベース局との相互通信を確立できる手段；

・前記料金計測手段により計算され送信される利用料金の支払いにあてるための価値単位を収容する前払い手段；

・各加入者に固有な所定のセット・ベース・マスターキーの助けを得てセット認証関数を実現することができる第一のセット認証手段；

－次のものを含む認可センター：

・前記格納マスターキーの助けを得て暗号化／復号関数を実現できる第二の暗号化／復号手段；

・前記セット・ベース・マスターキーの助けを得てセット認証関数を実現できる第二のセット認証手段。

【０００４】

【発明が解決しようとする課題】例えば、無線電話への応用の場合、独立セットは、第一および第二のセット認証手段を用いて独立セットに関する加入者の識別を認証するための操作が完了した後、交換電話ネットワークの有料サービスにアクセスする。

【０００５】独立セットに対する加入者の識別認証が、独立セットと認可センター間で、ランダム数、および、各加入者の固有のセット・ベース・マスターキーの助けを得たセット認証関数によるこのランダム数の変換、を

交換する能動的な認証であるのは好ましい。

【０００６】しかし、このような認証は、加入者を認証し、この加入者が交換電話ネットワークの有料サービスにアクセスするのを認可することができるだけである。

【０００７】それは、このように識別されアクセスが認可された加入者と「会話」する設備に関して、利用料金の支払いに役立つ前払い手段が通信の継続中、すべてを包括しているという保証を可能にすることはない。

【０００８】本出願人による１９９０年１０月１０日付けのフランス国特許出願第９０１２５１０号は、第一および第二のセット認証手段の助けを得て、通信の継続中利用料金の能動的認証を用いることにより、この問題に対する解決を提供した。

【０００９】この利用料金の能動的な認証は特に次のことを可能にする：

－料金計測手段により無線電話インタフェースを介して前払い手段へ送信された利用料金の証明；

－それらの利用料金が正しく受信され理解されたことの実証；

－それらが実際に前払い手段から差し引かれたことの実証。

【００１０】更に、前払い手段の勘定に所定の数の価値単位を再ロードするための手続きが知られている。

【００１１】これらの手続きは、一般的に通信それ自体の外部で、ローカルに、例えば、認可センターで直接に、あるいは認可センターと何の連結もない「オフライン」の独立セットにおいて、あるいは遠隔的に、例えば、ミニテル（MINITEL 、商標）サーバーによる遠隔ローディングのような特定のアプリケーションを介して、発生する。しかし、後者の手続きの場合、遠隔ロードされた量の適切な受信の保証や、独立セットによるその遠隔ローディングが拒絶されないという保証がない。

【００１２】更に、前払い手段の遠隔ローディングは、前払い手段を発行しあるいは管理する認可センターとは異なる、そして独立セットが商業的に所属しない、第三者の認可センターにより加入者がチェックされる時に必要とされるかもしれない（これは、例えば、加入者が自分の独立セットをその管理に責任を持つ運営者とは異なる運営者によりカバーされる区域において利用する場合、つまり、ＧＳＭアプリケーションにおけるいわゆる「ぶらつき（ROAMING）」サービスの場合がそうである。

【００１３】この状況において、第三者の認可センターの側の主導で行なう前払い手段の遠隔ローディングという解決策は安全性の点で満足すべきものではない。

【００１４】実際、遠隔ローディング依頼およびその量に関する秘密性および保全性は保証されないので、欺瞞的な再生が可能かもしれない。

【００１５】本発明はこの問題に対する解決を提供する。

【００１６】それで、本発明の目的は、独立セットが商業的に所属しないアクセス・システム（ＧＳＭアプリケーションではいわゆる「ぶらつき」サービス）に加入者がアクセスする場合でも、遠隔ローディングの依頼およびその量の秘密性および保全性を確保することのできる遠距離通信設備を提供することである。

【００１７】本発明の目的は、また、このようにアクセスされるアクセス・システムに関して、遠隔ローディングの依頼およびその量が正しく受信され理解されたこと、そして前払い手段の単位メーターがこのように遠隔ロードされた価値単位の数を実際に再ロードされたことを保証することである。

【００１８】本発明の目的は、最後に、加入者による遠隔ローディング依頼が拒絶されないことを保証する前払い手段の安全な遠隔ローディングの方法を提供することである。

【００１９】

【課題を解決するための手段】本発明は上述のタイプの遠距離通信設備からスタートする。

【００２０】本発明の最初の特徴によれば、独立セットは更に次のものを有している：

－セット・ベース・マスターキーの助けを得て生成関数を確立することができる第一の生成手段；

－セット・ベース・マスターキーの助けを得て生成関数による所定のワードの変換である遠隔ローディング・マスターキーの助けを得て遠隔ローディング関数を確立できる第一の遠隔ローディング手段。

【００２１】アクセス・システムは更に次のものを有している：

－所定の遠隔ローディング依頼に応じて所定の数の価値単位を発行でき、また遠隔ローディング・マスターキーの助けを得て遠隔ローディング関数を確立することができる第二の遠隔ローディング手段；

－所定のシステム・ベース・マスターキーの助けを得てシステム認証関数を確立することができる第一のシステム認証手段。

【００２２】認可センターは更に次のものを有している：

－システム・ベース・マスターキーの助けを得てシステム認証関数を確立できる第二のシステム認証手段；そして、

－セット・ベース・マスターキーの助けを得て生成関数を確立できる第二の生成手段。

【００２３】本発明の設備は、更に、遠隔ローディング・モードを含んでおり、そのモードにおいては、独立セットから発せられる所定の数の価値単位に対する遠隔ローディング要請ワードに応じて、第一および第二のセット認証手段および第一および第二のシステム認証手段は、独立セットから発せられるセット認証ワードと、セット・ベース・マスターキーの助けを得てセット認証関数により得られるこのワードの変換どをそれぞれ交換することにより、また、認可センターから発せられるシステム認証ワードと、システム・ベース・マスターキーの助けを得てシステム認証関数により得られるこのシステム認証ワードの変換を交換することにより、独立セットおよびアクセス・システムのそれぞれの能動的な認証を実行する。

【００２４】アクセス・システムおよび独立セットの認証がチェックされる場合、第二の生成手段は、認可センターのレベルで、遠隔ローディング要請ワードの変換（セット・ベース・マスターキーの助けを得て生成関数により得られる）である遠隔ローディング・マスターキーを計算する。

【００２５】認可センターのレベルでの遠隔ローディング・マスターキーの生成の場合、第二の暗号化／復号手段が暗号化されたローディング・マスターキーを格納マスターキーの助けを得て第一の暗号化／復号手段に送信し、第一の暗号化／復号手段は、アクセス・システムのレベルで格納することを目的としてそれを復号する。

【００２６】遠隔ローディング・マスターキーがアクセス・システムに格納される場合には、安全な方法で価値単位の数を前払い手段に遠隔ロードする目的で、第一および第二の遠隔ローディング手段が遠隔ロードされるべき価値単位の数に関する遠隔ローディング要請ワード、ならびに、遠隔ローディング・マスターキーの助けにより得られる該遠隔ローディング要請ワードの遠隔ローディング関数による変換を交換する。

【００２７】このような設備は、第一の操作者により前払い手段が引き渡された加入者で、第二の操作者によりチェックされながら「動き回る」加入者が任意の時点で自分の前払い手段に遠隔ロードすることを可能にするので有利である。更に、遠隔ローディングは動的に、安全にそして適切なら通信を中断することなく行なえる。

【００２８】所定の数の価値単位の遠隔ローディングに対する要請が電話通信の外部において、加入者の要請により行なわれれば有利である。

【００２９】変形として、所定の数の価値単位の遠隔ローディングの要請が電話通信の際に行なわれるようにすることもできる。

【００３０】本発明はまた、上述のタイプの遠隔ローディング・モードに依存する前払い手段の安全な遠隔ローディングのための方法に関するものである。

【００３１】本発明の他の特徴および有利な点は以下の説明ならびに添付図面から明らかにされるであろう。

【００３２】

【実施例】図１において、既知のタイプの無線電話設備は、移動可能な独立電話加入者アクセス・システムＳＡＡを、複数の移動あるいは固定独立セットＰＡと協働するように配置している。

【００３３】アクセス・システムＳＡＡは複数のベース

局ＢＦを含み、ベース局の各々は交換電話ネットワークＲＴＣに連結されている。

【００３４】本発明の理解を容易にするために、図１では独立セットＰＡおよびベース局ＢＦがそれぞれ一つずつしか示されていない。

【００３５】各独立セットＰＡは最も近いベース局ＢＦと無線電話による相互通信を確立するための手段ＭＥを有している。

【００３６】アクセス・システムＳＡＡに接続された認可センターＣＡは、後でより詳細に説明するが、アクセス・システムと独立セットとの間の通信を監督しチェックする。

【００３７】この種の設備は、例えばＧＳＭに適用されているが、L'ECHO DES RECHERCHES誌、No. 131 、１９８８年、第一季号、５－１６ページ、B. GHILLEBERT, P. COMBESCURE, A. MALOBERTI の記事、および同じ雑誌の No. 139、１９９０年、第一季号、１３－１９ページ、P. JOLIE, G. MAZZIOTTO の記事に説明されている。

【００３８】実際的には、アクセス・システムのレベルでは、ベース局ＢＦに連結された操作手段が設けられており、この操作手段は交換電話ネットワークＲＴＣの有料サービスの利用に対する料金を計算できる料金計測手段ＭＧを有している。

【００３９】独立セットＰＡの側では、前払い手段ＭＰＡＹを有しており、この前払い手段ＭＰＡＹは遠隔的に再ロードすることができ、処理装置（図示されていない）およびメモリ（図示されていない）を備え、メモリは料金計測手段により計算され送信される利用料金の支払いにあてるための価値単位を収納することができる。

【００４０】実際的には、メモリは外界からのふさわしくない時期になされるデータの直接書き込みに対し保護されている。

【００４１】ＧＳＭへ適用する場合、前払い手段ＭＰＡＹが、独立セットＰＡの無線相互通信を確立するための手段ＭＥと協働する着脱可能な加入者識別モジュールＳＩＭに収納されているのは有利である。

【００４２】前払い手段ＭＰＡＹのメモリがＥＰＲＯＭあるいはＥＥＰＲＯＭタイプのもので、ＳＩＭモジュールの処理装置により正しく保護されているのは好ましい。

【００４３】ＳＩＭモジュールは標準的なＩＳＯタイプのカードに収納されている。

【００４４】変形として、ＳＩＭモジュールを無線相互通信を確立するための手段ＭＥにプラグで差し込まれるコンポーネントとすることもできる。

【００４５】フランス国特許出願第９０１２５１０号に記載されているように、独立セットのレベルでは、所定のセット・ベース・マスターキーＳＢの助けを得てセット認証関数Ａを確立することができる第一のセット認証手段ＡＵＰＡが設けられており、認可センターＣＡのレベルでは、前記セット・ベース・マスターキーＳＢの助けを得てセット認証関数Ａを確立できる第二のセット認証手段ＡＵＰＡＣＡが設けられている。

【００４６】前記特許出願においては、第一および第二のセット認証手段ＡＵＰＡおよびＡＵＰＡＣＡは相互通信の間、利用料金の認証のために役立つことに注目すべきである。

【００４７】ＧＳＭへの適用においては、セット・ベース・マスターキーＳＢは、例えば、各加入者に固有で例えば１２８ビット長の秘密マスターキーである。

【００４８】セット認証関数Ａに関して言えば、それは例えばＤＥＳ (DATA ENCRYPTION STANDARD) タイプの暗号関数である。

【００４９】既知のように、アクセス・システムＳＡＡは、また、第一の暗号化／復号手段ＭＡＣＳＡＡが設けられており、それにより、格納マスターキーＫＣあるいはＦＡの助けにより暗号関数ＡＣあるいはＦＣが確立される。

【００５０】上述のように、本発明の目的は前払い手段の遠隔ローディングのための安全な手続きを提供することである。

【００５１】この目的を達成するために、本発明の設備は、独立セットＰＡのレベルでは、セット・ベース・マスターキーＳＢの助けを得て生成関数ＡＧを確立できる第一の生成手段ＡＧＰＡ、および、遠隔ローディングマスターキーＫＣＨあるいはＰＣＨ（これはセット・ベース・マスターキーＳＢの助けを得た生成関数ＡＧの変換である）の助けを得て遠隔ローディング関数ＡＣＨあるいはＦＣＨを確立できる第一の遠隔ローディング手段ＡＣＨＰＡを備えることにより完成される。

【００５２】つりあいとして、アクセス・システムＳＡＡのレベルでは、本設備は、所定の数の価値単位ｎを発行し、遠隔ローディングマスターキーＫＣＨあるいはＰＣＨの助けを得て遠隔ローディング関数ＡＣＨを確立できる第二の遠隔ローディング手段ＡＣＨＳＡＡ、および、所定のシステム・ベース・マスターキーＫＯあるいはＳＯの助けを得てシステム認証関数ＡＯあるいはＦＯを確立できる第一のシステム認証関数ＡＵＳＡＡを備えることにより完成される。

【００５３】同じく、つりあい上、認可センターＣＡは、本発明により、更に、セット・ベース・マスターキーＳＢの助けにより生成関数ＡＧを確立できる第二の生成手段ＡＧＣＧおよび、システム・ベース・マスターキーＫＯあるいはＰＯの助けを得てシステム認証関数ＡＯあるいはＦＯを確立できる第二の認証手段ＡＵＳＡＡＣＡを有している。

【００５４】実際上、システム認証関数ＡＯあるいはＦＯ、セット認証関数Ａ、暗号関数ＡＣあるいはＦＣ、遠隔ローディング関数ＡＣＨあるいはＦＣＨ、そして生成

関数ＡＧは、「ＤＥＳ」（DATA ENCRYPTION STANDARD）あるいは「ＲＳＡ」（RIVESTSHAMIR ADELMAN）などの暗号アルゴリズムに依存している。

【００５５】これらＤＥＳあるいはＲＳＡアルゴリズムは読み出し専用メモリに格納される。

【００５６】ＤＥＳ暗号アルゴリズムは秘密ベース・マスターキーにより運営されることを思い起こすべきである。同様に、本設備の要素がＤＥＳの助けで会話できるためには、秘密マスターキーが会話する両方の要素に同時に格納されていなければならない。

【００５７】これとは対照的に、ＲＳＡアルゴリズムは、実際には二つの互いに依存するマスターキー（すなわち、一つは二つの会話する要素のうちの一つに格納される公開マスターキー、もう一つは二つの要素の他の一つに格納される秘密マスターキー）の組合わせであるベース・マスターキーの助けで運営される。

【００５８】例えば、システム認証関数ＡＯがＤＥＳアルゴリズムに依存する場合、秘密システム・ベース・マスターキーＫＯがシステムＳＡＡのレベルで認証手段ＡＵＳＡＡに格納されると共に、認可センターＣＡのレベルで認証手段ＡＵＳＡＡＣＡに格納される。

【００５９】このように、システム・ベース・マスターキーＫＯの助けを得たシステム認証関数ＡＯによるランダム数Ｓの変換ＲＥＳＳは次のように書ける：

ＲＥＳＳ＝ＡＯ（ＫＯ，Ｓ）

これとは対照的に、システム認証関数ＦＯがＲＳＡアルゴリズムに依存する場合には、秘密システム・ベース・マスターキーＳＯはアクセス・システムＡＵＳＡＡレベルでのみ格納され、公開システム・ベース・マスターキーＰＯは認可センターＣＡレベルで格納される。このように、秘密マスターキーＳＯの助けを得たシステム認証関数ＦＯによるランダム数Ｓの変換ＲＥＳＳは次のように書ける：

ＲＥＳＳ＝ＳＯ（Ｓ）

他方、認可センターレベルで、システム認証手段ＡＵＳＡＡＣＡは、公開システム・ベース・マスターキーＰＯの助けを得て、システム認証関数ＦＯによりワードＲＥＳＳの変換を計算する。

【００６０】アクセス・システムＳＡＡの認証の立証は次のように書くことができる：

ＰＯ（ＲＥＳＳ）＝？（Ｓ）

上の各式は、以下になされる本発明の遠隔ローディング手続きの詳細な説明において役に立つ。

【００６１】ＲＳＡあるいはＤＥＳ暗号アルゴリズムは商業的に市場で流通しているアルゴリズムである。

【００６２】本発明の安全遠隔ローディング手続きは二つの部分に分かれる。

【００６３】第一部分はアクセスされるアクセス・システムと前払い手段を管理する責任を負う認可センターとの間の交渉ステップからなっている。

【００６４】簡単に言えば、それは独立セット、および認可センターとの関係におけるアクセス・システムの認証が関係している。独立セットおよびアクセス・システムの認証がチェックされれば、認可センターはアクセス・システムに一時的遠隔ローディング・マスターキーを提供し、それによりアクセス・システムは前払い手段との関係で自分自身の認証が可能とする。

【００６５】第二部分は、次に、遠隔的にそして安全に所定の数の価値単位をロードするために、アクセス・システムと前払い手段との間で生じる。

【００６６】以下、図２および図３を参照して、本発明による遠隔ローディング手続きの第一部分を詳細に説明する。

【００６７】実際上、前払い手段ＭＰＡＹのために、アクセスされるアクセス・システムＳＡＡは、相互通信の間、利用できるクレジット（利用できる単位数および使用される貨幣単位）を利用する。

【００６８】例えば、この価があるしきい値に到達あるいは超えた場合（ステップ１０）、アクセス・システムはセット認証ワードＲ０を生成し（ステップ１２）、このセット認証ワードＲ０を独立セットに送る。

【００６９】このセット認証ワードＲ０に応じて、独立セットは幾つかの解決に直面する。

【００７０】まず第一に、前払い手段がアクセス・システムに属する場合。この場合、アクセス・システムがその前払い手段に遠隔ロードするために必要な情報を所有している。

【００７１】第二に、アクセス・システムが認められている認可センターに前払い手段が属する場合。そのアクセス・システムは、それゆえ、前払い手段の遠隔ローディングのために必要な情報を所有する。

【００７２】第三に、認可センターが認定していないアクセス・システムがアクセスされ、その認可センターに前払い手段が属する場合。アクセスされるそのアクセス・システムは、遠隔ローディングに必要な情報を得るために前払い手段の発行当局に接触しなければならない。

【００７３】本発明による遠隔ローディング手続きが関係しているのは、この第三の状況であり、次のものを設定する必要がある：

－アクセス・システムと認可センターの間の相互の認証のメカニズム；－交換される秘密情報の秘密保護に関するメカニズム；そして、－拒絶しないためのメカニズム。

【００７４】このように、頻繁にやりとりのあるアクセス・システムが認められていない当局に前払い手段が属し、独立セットが前払い手段のクレジットのレベルにおいてしきい値を超過したことを通知される場合、前払い手段はｎ価値単位の遠隔ローディングの要請（これは遠隔ローディング要請ワードＲとも呼ばれるランダム数を生成することである）を行ない、このランダム・ワード

Ｒをアクセス・システムＳＡＡに送り返す。

【００７５】次に、ステップ１６において、第一のセット認証手段は、セット・ベース・マスターキーＳＢの助けを得てセット認証関数Ａによりセット認証ワードＲ０の変換ＲＥＳ０を計算する。この変換ＲＥＳ０の計算には要請された価値単位の数ｎも関与している。

【００７６】ステップ１６が完了すると、遠隔ローディング要請ワードＲ、変換ＲＥＳ０および価値単位の数ｎがアクセス・システムＳＡＡに送られる。　これらのワードＲ、ＲＥＳ０およびｎに応じて、アクセス・システムはクレジット認証要請を行なう（ステップ１８）。このクレジット認証要請とは、クレジット認証要請ワードＲ１を生成し、ワードＲ１、Ｒ、Ｒ０、ＲＥＳ０およびｎを認可センターＣＡに送る（ステップ２０）ことである。

【００７７】これらのワードに応じて、認可センターはシステム認証要請を行なう（ステップ２２）。これは、システム認証ワードＲ２を生成し、このシステム認証ワードＲ２をアクセス・システムＳＡＡに送ることである。　アクセス・システムおよび認可センターの相互の認証は第一および第二のシステム認証手段ＡＵＳＡＡおよびＡＵＳＡＡＣＡにより担われる（ステップ２２、２４、２６）。

【００７８】ステップ２４において、システム認証関数はＤＥＳタイプの暗号アルゴリズムに依存するものとすることができる。その場合、ステップ２４は秘密システム・ベース・マスターキーＫＯの助けを得て認証関数ＡＯによりワードＲ２の変換ＲＥＳ２を計算する。

【００７９】これとは対照的に、システム認証手段がＲＳＡタイプの暗号アルゴリズムに依存する場合、システム認証手段は、システムＳＡＡレベルで格納されている秘密マスターキーＳＯの助けを得て、システム認証ワードＲ２の変換ＲＥＳ２を計算する。

【００８０】ステップ２４で、価値単位の数ｎが変換ＲＥＳ２の計算に関与していることに注目すべきである。

【００８１】最後に、ステップ２４が完了すると、アクセス・システムＳＡＡは変換ＲＥＳ２を認可センターに送る。

【００８２】認可センターＣＡのレベルで、セットＰＡの認証およびシステムＳＡＡの認証がチェックされる。

【００８３】セットの認証のチェックについては、セット・ベース・マスターキーＳＢの助けを得て、セット認証関数ＡによりＲＥＳ０’が計算（ステップ２６）され、また、このように計算された変換ＲＥＳ０’と受け取られた変換ＲＥＳ０との比較が行なわれる。

【００８４】システム認証のチェックに関しては、マスターキーＫＯの助けによりシステム認証関数ＡＯによりＲＥＳ２’が計算され（ステップ２８）、また、このように計算された変換ＲＥＳ２’と受けてられた変換ＲＥＳ２との比較が行なわれる。ステップ２８は、システム認証手段がＤＥＳタイプのアルゴリズムに基づいている場合について示されている。

【００８５】これとは対照的に、システム認証手段がＲＳＡアルゴリズムに依存している場合には、ステップ３０において、システムワードＲ２の認証の立証のために、認可センターレベルで格納されている公開マスターキーＰＯにより変換ＲＥＳ２の解読の計算が行なわれる。

【００８６】独立セットおよびシステムの認証が立証されると、遠隔ローディング・マスターキーの計算が行なわれる（ステップ４０）。遠隔ローディング・マスターキーがＤＥＳタイプのアルゴリズム秘密マスターキーである場合には、遠隔ローディング・マスターキーＫＣＨは、マスターキーＳＢの助けを得て生成された関数ＡＧによるクレジット要請ワードＲの変換である（ステップ４２）。

【００８７】対照的に、ＲＳＡタイプのアルゴリズムの場合は、マスターキーＳＢの助けを得て生成するための関数ＡＧにより、公開マスターキーＰＣＨおよび秘密マスターキーＳＣＨからなるマスターキーの組（ＰＣＨ，ＳＣＨ）を得ることができる（ステップ４４）。公開マスターキーＰＣＨはアクセス・システムＳＡＡのレベルで格納される。

【００８８】遠隔ローディング・マスターキーＫＣＨあるいはＰＣＨが認可センターレベルで生成されると、この遠隔ローディング・マスターキーＫＣＨあるいは適切な場合にはこの遠隔ローディングマスターキーの公開部分ＰＣＨを暗号化してアクセス・システムに送信するのは適切である。

【００８９】遠隔ローディング・マスターキーＫＣＨあるいはＰＣＨの暗号化はＤＥＳタイプの暗号アルゴリズムあるいはＲＳＡタイプの暗号アルゴリズムの助けにより実行できる。

【００９０】ＤＥＳタイプの暗号アルゴリズムの場合には、認可センターＣＡレベルおよびアクセス・システムＳＡＡレベルで格納マスターキーを利用するのは適切である。

【００９１】例えば、格納マスターキーＫＣは、システム・ベース・マスターキーＫＯの助けによる暗号関数ＡＧＣによるワードＲ１の変換である（ステップ４６および４７）。

【００９２】次いで、遠隔ローディング・マスターキーＫＣＨの暗号化ＥＫＣＨ（ステップ４８）が、アクセス・システムＳＡＡおよび認可センターＣＡのレベルで利用できる秘密格納マスターキーＫＣの助けにより暗号関数ＡＣにより実行される。

【００９３】変形として、遠隔ローディング・マスターキーＰＣＨの暗号化は、秘密格納マスターキーＫＣの助けを得て、暗号化関数ＡＣにより実行される。

【００９４】対照的に、ＲＳＡタイプの暗号化／復号ア

ルゴリズムの場合には、認可センターCAのレベルで公開マスターキーFA、アクセス・システムSAAのレベルで秘密マスターキーを利用するのが適切である。

【0095】遠隔ローディング・マスターキーKCHの暗号化EKCH（ステップ50）が次いで公開マスターキーFAの助けで実行される。

【0096】変形として、次いで、遠隔ローディング・マスターキーPCHの暗号化EPCHが、公開マスターキーFAの助けで実行される。

【0097】暗号化が行なわれると、マスターキーEKCHあるいはEPCH（ステップ52）がアクセス・システムSAAに送られ、アクセス・システムの側ではこのように暗号化されて受け取ったマスターキーを解読する。

【0098】暗号化／復号手段が適切に配置された当然の帰結として、マスターキーKCHあるいはPCHの復号が、ステップ54、56、58、60に記載された式に従って適切になされる。

【0099】次に、前払い手段の遠隔ローディングの第二部分に関して図4を参照する。

【0100】遠隔ローディングは、前払い手段の遠隔ローディングに責任を負うアクセス・システムSAAの料金計測手段と独立セットPAとの間で発生する。

【0101】先に詳細に述べたように、アクセス・システムSAAは遠隔ローディング関数ACHならびに一時的遠隔ローディング・マスターキーKCHあるいはPCHを利用する。

【0102】独立セットおよびアクセス・システムの認証、マスターキーKCHあるいは（PCH，SCH）の生成、それの暗号化とアクセス・システムへの送信、およびそのマスターキーの暗号化が完了すると、最後に前払い手段の遠隔ローディングの手続が実施される。

【0103】独立セットもまた本質的に遠隔ローディング・マスターキーKCHあるいは（PCH，SCH）を利用することに注意されたい（ステップ100、102）。

【0104】アクセス・システムSAAは要請された価値単位の数nの関数として遠隔ロードされる量C1を確立する（ステップ104）。

【0105】アクセス・システムは、マスターキーKCHあるいは公開マスターキーPCHの助けを得て遠隔ローディング関数ACHを用いて、量C1に依存して、遠隔ローディング要請Rの変換RESを計算する（ステップ106）。

【0106】遠隔ローディング関数ACHはRSAタイプのアルゴリズム（PCH，SCH）あるいはDESタイプのアルゴリズム（秘密マスターキーKCH）に依存することに注意すべきである。

【0107】関数ACHにより変換RESを計算した後、アクセス・システムSAAは受信要請ランダム・ワードR3を生成し（ステップ108）、変換RES、量C1およびランダム・ワードR3を独立セットPAに送信する（ステップ110）。

【0108】独立セットの側では、DESタイプのアルゴリズムの場合、変換RES'を計算し（ステップ112）、RSAタイプのアルゴリズムの場合には、秘密遠隔ローディング・マスターキーSCHのもとでRESおよびワードRの変換を計算することにより（ステップ114）、システムSAAの署名を実証する。

【0109】システムSAAの認証の場合には、新たなクレジットC2の計算が行なわれる（ステップ116）。

【0110】次いで、前払い手段は、選択された暗号アルゴリズムに応じて、新たなクレジットC2にマスターキーKCHおよびランダム・ワードR3で署名し（ステップ118）、あるいはマスターキーSCHおよびランダム・ワードR3で署名する（ステップ120）。

【0111】最後に、ステップ122において、新たなクレジットC2および変換RES3が送信される。

【0112】アクセス・システムの側では、DESタイプのアルゴリズムの場合はRES3'を計算することにより遠隔ローディングの受け入れの認証を実証し（ステップ126および128）、RSAタイプのアルゴリズムを使用する場合には変換RES3の認証を実証してそれを行なう（ステップ124）。

【0113】遠隔ローディング要請ワードRとその変換RESを交換する前に、遠隔ローディング依頼の認可の認証を得ることを希望して、システム認証手段AUSAAおよびAUSAACAが認可認証ワード（ステップ118、図2）およびシステム認証関数KO、SOによるその変換RES1を交換するのは有利である。

【0114】アクセス・システムと認可センターとの間で拒絶が無いことは、一時的遠隔ローディングマスターキーKCHあるいは（PCH，SCH）を用いる原理により保証される。それで、管理当局は、遠隔ローディングの運営に役立つ遠隔ローディング・マスターキーを供給することのできる唯一のものであるため、遠隔ローディングを認可しなければならないのにそれを断るということはできない。

【0115】他方、アクセス・システムは、遠隔ローディングの認可が遠隔ローディング・マスターキーと結び付けられるときにのみ有効であれば、遠隔ローディングの認可の受け入れを主張することはできない。

【0116】GSMに適用する場合、遠隔ローディング手段ACHPAおよび生成手段AGPAを着脱可能な加入者識別モジュールSIMに収容するのは有利である。

【0117】加入者識別モジュールSIMを利用するGSMの適用において本発明を実行するためには、このモジュールに前払いアプリケーションが存在する必要がある。

【０１１８】この前払いアプリケーションは非占有の読み取りファイルおよび遠隔ローディング・マスターキーKCHあるいは（PCH，SCH）を提示することにより更新（アプデート）がプロテクトされている必要がある。

【０１１９】この遠隔ローディング・マスターキーKCHあるいは（PCH，SCH）は一時的なものであり頻繁にやりとりする当局が、SIMモジュールのメモリに追加されるべきクレジットの価値を提示することにより、前払いファイルに価値を書き込むことを可能にするものである。

【０１２０】SIMモジュールを使用するGSMアプリケーションでは、無線電話相互通信を確立するための手段MEが、通信している加入者識別モジュールSIMに対し、先述の遠隔ローディングの提案ROを送信し、次いで、一時的遠隔ローディング・マスターキーKCHあるいは（PCH，SCH）により証明された、遠隔ロードされるべき量を含むワードC1を送信する。

【０１２１】GSMアプリケーションの場合、第一の遠隔ローディング手段および第一の生成手段はSIMモジュールにある。

【０１２２】モジュールが無線通信運営者により発行される場合、アクセス・システムSAAはVLR（ビジタ配置レジスタ VISITOR LOCATION REGISTER）のレベルに配置され、認可センターCAはHLR（ホーム配置レジスタ HOME LOCATION REGISTER ）のレベルに配置される。

【０１２３】交換電話ネットワークのレベルでは、前払いアプリケーションを収容するSIMモジュールは、名目上の配置レジスタに関連する加入者識別番号IMにより識別される。

【０１２４】通信の間には、SIMモジュールはVLRレジスタのレベルに配置される。

【０１２５】それで、本発明によれば、SIMモジュールの使用に対する料金の請求を引き受けるのはVLRレジスタである。

【０１２６】VLRレジスタは任意の時点において残っている前払い手段のクレジットを知っていることに注意すべきである。

【０１２７】このように、クレジットが所定のしきい値に達すると、レジスタVLRはモジュールSIMに対する遠隔ローディングを提案する際に、モジュールSIMに知らせる。

【０１２８】この情報に応じて、SIMはランダム数Rを生成し、このランダム数RによりSIMモジュールの能動的な認証が可能になり、図２および図３を参照して説明したように、一時的再ローディング・マスターキーKCHあるいは（PCH，SCH）を生成するように要請する。

【０１２９】これと同時に、レジスタVLRはレジスタHLRとの関係で正当性が確認され、それに対して一時的遠隔ローディング・マスターキーを要請する。

【０１３０】次にVLRとSIMとの間の遠隔ローディングの実施をチェックするために使用されるのは、この遠隔ローディング・マスターキーである。 例としてあげると、ワードR、R0、R1、R2、R3は１２８ビット長のランダム・ワードとすることができる。遠隔ロードされるべき価値および前払いモジュールで利用できる量C1およびC2は４ビット長である。

【０１３１】マスターキー・ワードRES0は３２ビット長である。

【０１３２】マスターキー・ワードRES、RES1、RES2およびRES3は１２８ビット長のワードである。

【０１３３】マスターキーKOおよびKCは１２８ビット長のマスターキーであり、遠隔ローディング・マスターキーKCH、（PCHあるいはSCH）は選択される暗号アルゴリズムのタイプに依存して６４ビットないし５１２ビットの範囲で変化することができる。

【０１３４】本発明は独立セットとアクセス・システムの間の無線タイプの相互通信に限定されないことに注意されたい。

【０１３５】実際、本発明は任意の通信ネットワークに関係する。このように、本発明は次のものを用いる装置に適用できる：

－アクセス・システムとの無線連結を備えた移動式あるいは固定式の個人用独立セット；

－アクセス・システムとの有線あるいは無線連結を備えた固定公衆独立セット；

あるいは、

－アクセス・システムとの有線連結を備えた移動式あるいは固定式個人用独立セット。

【０１３６】このように任意の通信ネットワークに一般的に適用できるということは、本発明の遠隔ローディングのモードが独立セットとアクセス・システムの連結の違いにより影響されないという事実により説明される。

【０１３７】実際的には、無線電話設備の場合（図１－図４）、独立セットの相互通信モジュールMEはアクセス・システムSAAのベース局BFと会話する無線モジュールである。

【０１３８】対照的に、有線タイプの電話設備に関しては、独立セットの相互通信モジュールMEは、電話ネットワーク接続装置（例えば、公衆電話接続装置URPあるいはローカルな交換パネル）からなるベース局と会話する有線モジュールである。

【０１３９】本発明の遠隔ローディング手続きはUPT（Universal Personal Telecommunication）として知られるサービスによく適合することに注目されたい。

【０１４０】より正確に言えば、そのサービスは、特に各加入者が固有の個人識別番号により知られるという事

実により、そのサービスを提供する幾つかの通信ネットワークを横断して個人的に移動できる可能性を加入者に提供することができる。それで、有線タイプの通信ネットワークにおける移動の際には、加入者は自分の位置をいつでも利用センターに示すことを可能にする登録機能を利用する。

【０１４１】この結果、図１ないし図４を参照して説明した遠隔ローディング手続きにより、前払いアプリケーションに関してＵＰＴサービスを有利に補充することができる。

【０１４２】本発明の遠隔ローディング手続きはＵＰＴサービスを持たない有線ネットワークにも適用できることに注目すべきである。例えば、電話カードの文脈で述べれば、第一の運営者により管理されあるいは発行される電話カードにより、第二の運営者により管理される通信ネットワークへアクセスすること、およびその逆を認めるという契約を第一および第二の運営者間で結ぶことができる。

【図面の簡単な説明】

【図１】本発明による無線電話設備を示す略図である。

【図２】本発明による安全な遠隔ローディング手続きの第一部分を説明するフローチャートである。

【図３】本発明による安全な遠隔ローディング手続きの第一部分を説明するフローチャートである。

【図４】本発明による遠隔ローディング手続きの第二部分およびその認証を説明するフローチャートである。

【符号の説明】

ＡＣＨＰＡ　第一の遠隔ローディング手段
ＡＣＨＳＡＡ　第二の遠隔ローディング手段
ＡＧＰＡ　第一の生成手段
ＡＧＣＡ　第二の生成手段
ＡＵＰＡ　第一のセット認証手段
ＡＵＰＡＣＡ　第二のセット認証手段
ＡＵＳＡＡ　第一のシステム認証手段
ＡＵＳＡＡＣＡ　第二のシステム認証手段
ＢＦ　ベース局
ＣＡ　認可センター
ＭＧ　料金計測手段
ＭＰＡＹ　前払い手段
ＰＡ　独立セット
ＲＴＣ　交換電話ネットワーク
ＳＡＡ　アクセス・システム

【図１】

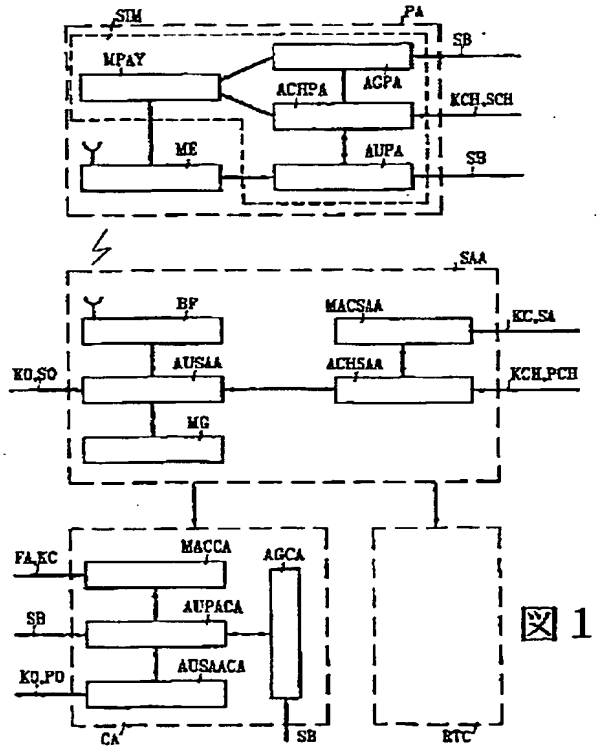


図１

【図2】

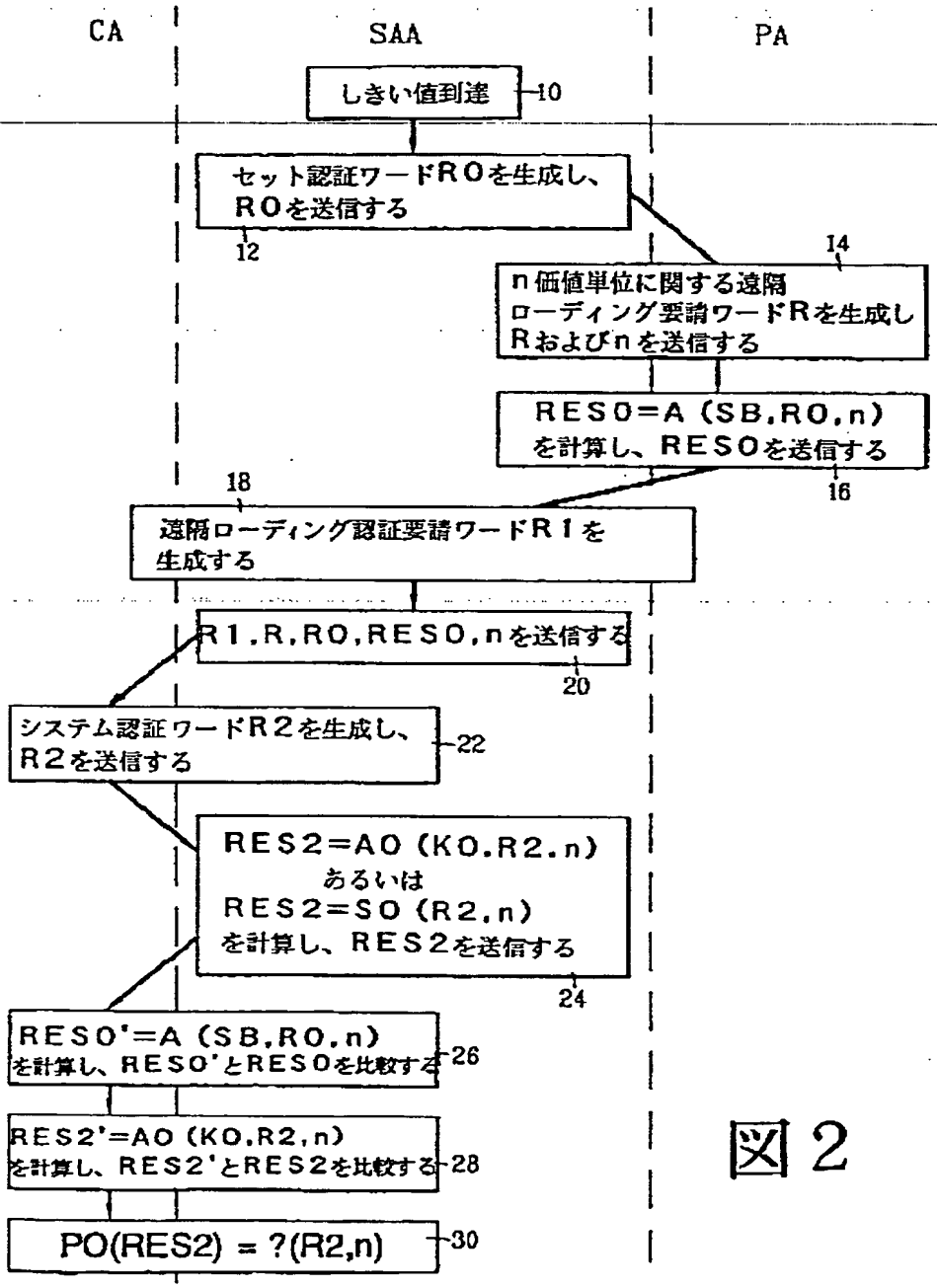

CA
SAA
PA
しきい値到達
10
セット認証ワードROを生成し、
ROを送信する
12
14
n価値単位に関する遠隔
ローディング要請ワードRを生成し
Rおよびnを送信する
RESO=A (SB,RO,n)
を計算し、RESOを送信する
16
18
遠隔ローディング認証要請ワードR1を
生成する
R1,R,RO,RESO,nを送信する
20
システム認証ワードR2を生成し、
R2を送信する
22
RES2=AO (KO,R2,n)
あるいは
RES2=SO (R2,n)
を計算し、RES2を送信する
24
RESO'=A (SB,RO,n)
を計算し、RESO'とRESOを比較する
26
RES2'=AO (KO,R2,n)
を計算し、RES2'とRES2を比較する
28
PO(RES2) = ?(R2,n)
30

図2

【図3】

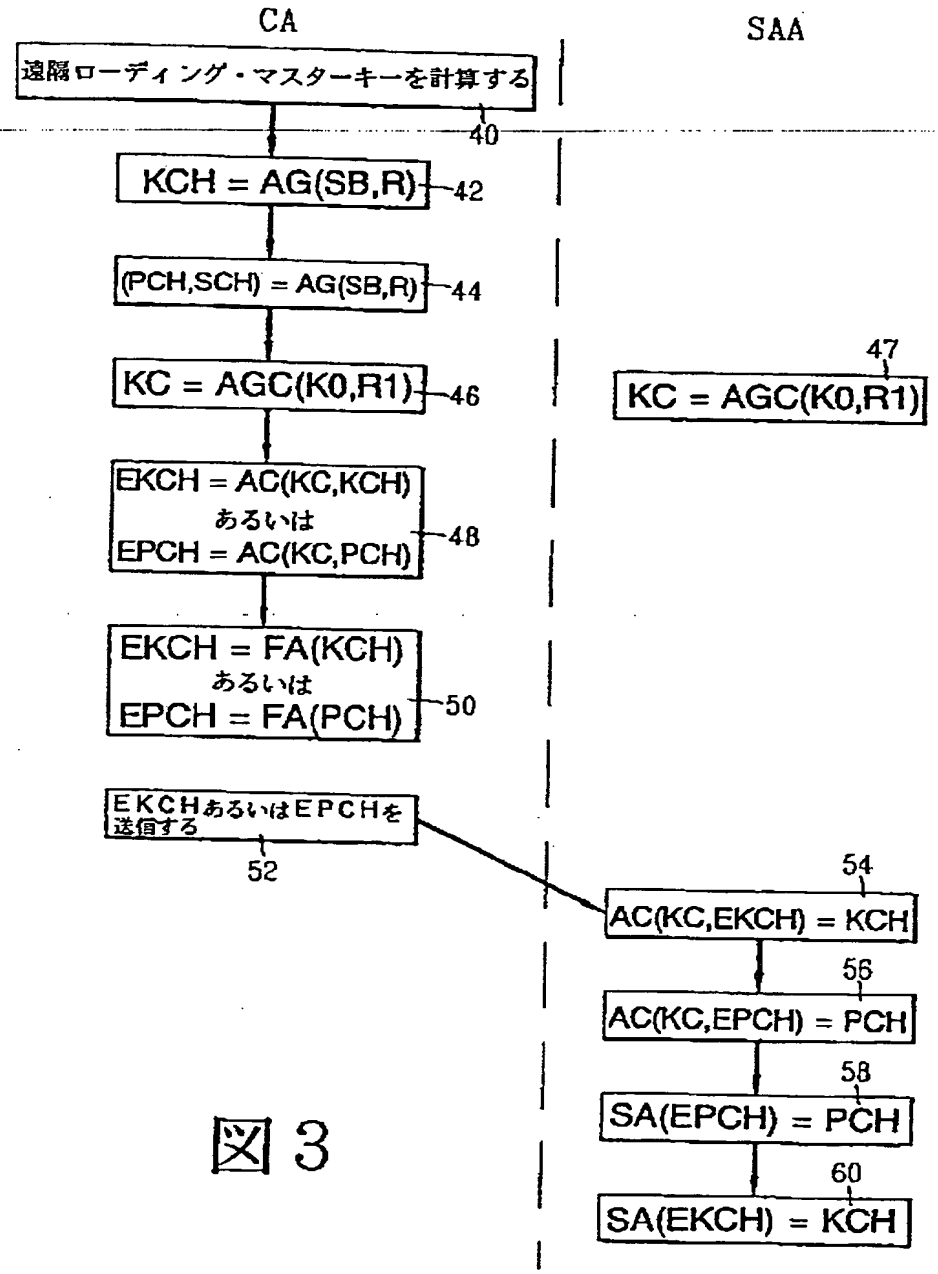

CA
SAA
遠隔ローディング・マスターキーを計算する
40
KCH = AG(SB,R)
42
(PCH,SCH) = AG(SB,R)
44
KC = AGC(K0,R1)
46
47
KC = AGC(K0,R1)
EKCH = AC(KC,KCH)
あるいは
EPCH = AC(KC,PCH)
48
EKCH = FA(KCH)
あるいは
EPCH = FA(PCH)
50
EKCHあるいはEPCHを送信する
52
54
AC(KC,EKCH) = KCH
56
AC(KC,EPCH) = PCH
58
SA(EPCH) = PCH
60
SA(EKCH) = KCH

図 3

【図4】

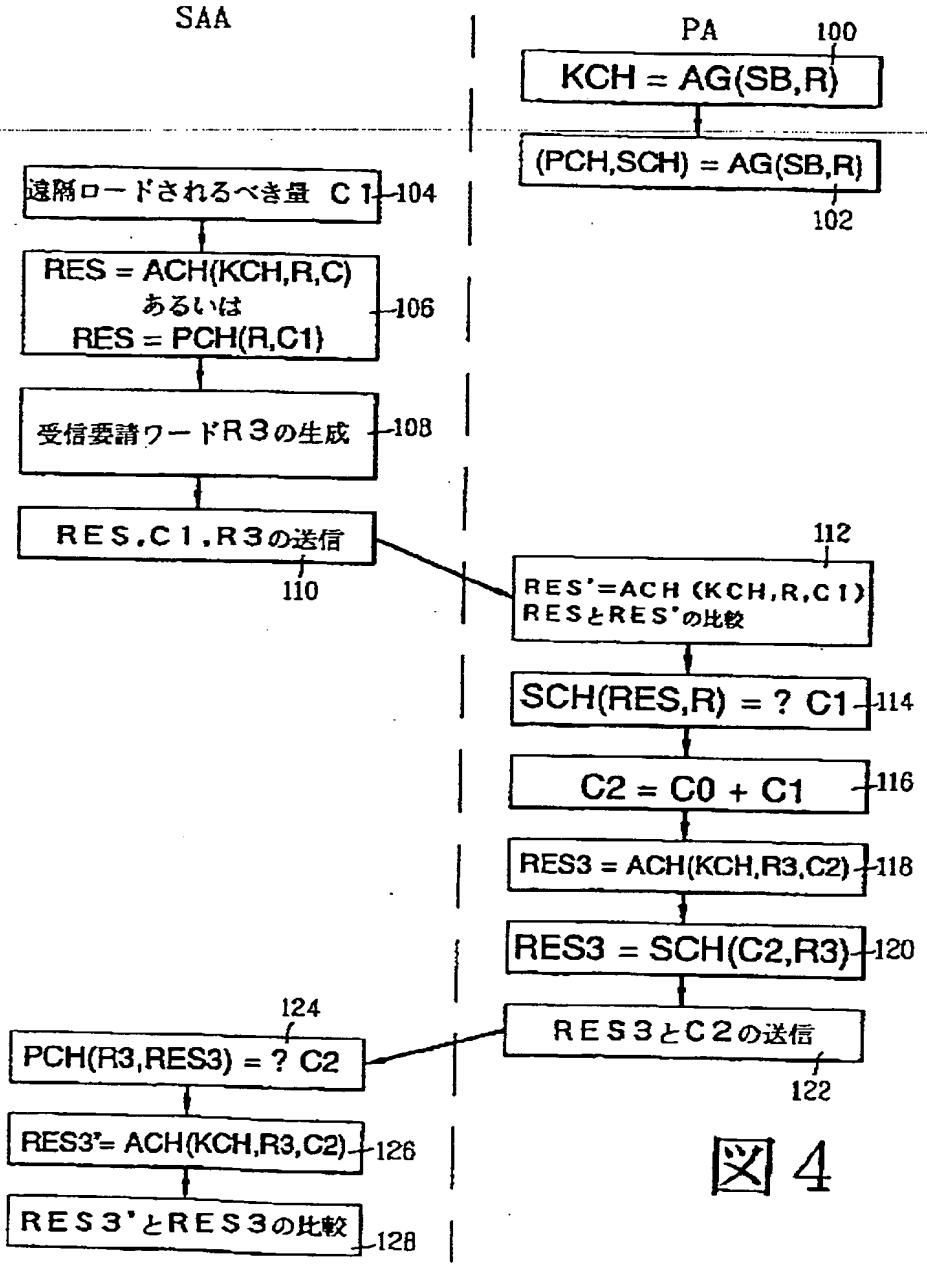


図4

フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
9/12				
H04Q 7/04		H 7304-5K		
		7117-5K	H04L 9/00	Z

(72)発明者　ローラ・ヌブ
フランス国、エフ－78990　エランクール、リュ・ド・モンモランシー、1
(72)発明者　フィリップ・ヨール
フランス国、エフ－14200　エルビーユ・サン・クレール、グランドデール、1201